Reliable Useful ISO-IEC-27001-Lead-Implementer Dumps & Leader in Qualification Exams & Correct PECB PECB Certified ISO/IEC 27001 Lead Implementer Exam

P.S. Free 2026 PECB ISO-IEC-27001-Lead-Implementer dumps are available on Google Drive shared by Dumpleader: https://drive.google.com/open?id=1k4JSwMubjd5JhjW34q1dVWQbA3tQTU4j

The web-based ISO-IEC-27001-Lead-Implementer practice exam is similar to the desktop-based software. You can take the web-based ISO-IEC-27001-Lead-Implementer practice exam on any browser without needing to install separate software. In addition, all operating systems also support this web-based PECB ISO-IEC-27001-Lead-Implementer Practice Exam. Both PECB Certified ISO/IEC 27001 Lead Implementer Exam practice exams track your performance and help to overcome mistakes. Furthermore, you can customize your PECB Certified ISO/IEC 27001 Lead Implementer Exam practice exams according to your needs.

To prepare for the PECB ISO-IEC-27001-Lead-Implementer certification exam, candidates can attend training courses offered by PECB or other authorized training providers. They can also study the ISO/IEC 27001 standard and related materials, such as the ISO/IEC 27002 standard, and practice implementing and managing an ISMS in a real-world setting. By passing the exam and obtaining the PECB Certified ISO/IEC 27001 Lead Implementer certification, professionals can demonstrate their expertise and commitment to information security management.

Topics covered by the PECB ISO IEC 27001 Lead Implementer Certification Exam:

ISO IEC 27001 Lead Implementer exam dumps cover the following topics of the ISO IEC 27001 Lead Implementer Certification Exam:

- Planning an ISMS implementation based on ISO/IEC 27001: 10%
- Preparing for an ISMS certification audit: 10%
- Implementing an ISMS based on ISO/IEC 27001: 20%
- Information security management system (ISMS): 20%
- Monitoring and measurement of an ISMS based on ISO/IEC 27001: 20%
- Continual improvement of an ISMS based on ISO/IEC 27001: 10%

PECB ISO-IEC-27001-Lead-Implementer Certification is highly valued by organizations as it demonstrates the ability of the certified professional to implement and manage an ISMS according to ISO/IEC 27001. PECB Certified ISO/IEC 27001 Lead Implementer Exam certification validates the knowledge and skills of the professional in information security management, risk management, and the implementation and maintenance of an ISMS. It also enhances the credibility of the professional and the organization they represent.

>> Useful ISO-IEC-27001-Lead-Implementer Dumps <<

Authorized ISO-IEC-27001-Lead-Implementer Pdf & Valid ISO-IEC-27001-Lead-Implementer Exam Pdf

The price of Our ISO-IEC-27001-Lead-Implementer exam questions is affordable and we provide the wonderful service before and after the sale to let you have a good understanding of our ISO-IEC-27001-Lead-Implementer study materials before your purchase and convenient download procedures in case you want to have a check on the ISO-IEC-27001-Lead-Implementer test. We have free demo on the web for you to know the content of our ISO-IEC-27001-Lead-Implementer learning guide. Once you have a try on our ISO-IEC-27001-Lead-Implementer trainng prep, you will know that our ISO-IEC-27001-Lead-Implementer practice engine contains the most detailed information for your ISO-IEC-27001-Lead-Implementer exam.

PECB Certified ISO/IEC 27001 Lead Implementer Exam Sample Questions (Q160-Q165):

NEW QUESTION # 160
Which of the following statements regarding information security risk is NOT correct?

- A. Information security risk cannot be accepted without being treated or during the process of risk treatment
- B. Information security risk can be expressed as the effect of uncertainty on information security objectives
- C. Information security risk is associated with the potential that the vulnerabilities of an information asset may be exploited by threats

Answer: A

Explanation:
According to ISO/IEC 27001:2022, information security risk can be accepted as one of the four possible options for risk treatment, along with avoiding, modifying, or sharing the risk12. Risk acceptance means that the organization decides to tolerate the level of risk without taking any further action to reduce it3. Risk acceptance can be done before, during, or after the risk treatment process, depending on the organization's risk criteria and the residual risk level4.

NEW QUESTION # 161
Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB. a document model database that offers high availability, scalability, and flexibility.
Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible. Fortunately. Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions.
To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access The implementation was based on all relevant agreements, legislation, and regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.
Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.
Based on scenario 3, what would help Socket Inc. address similar information security incidents in the future?

- A. Using cryptographic keys to protect the database from unauthorized access
- B. Using the access control system to ensure that only authorized personnel is granted access
- C. Using the MongoDB database with the default settings

Answer: A

Explanation:
In Scenario 3, the measure that would help Socket Inc. address similar information security incidents in the future is "B. Using cryptographic keys to protect the database from unauthorized access." Implementing cryptographic controls, including cryptographic key management, is a proactive measure to secure the data in the MongoDB database against unauthorized access. It ensures that even if attackers gain access to the database, they cannot read or misuse the data without the appropriate cryptographic keys. This approach aligns with best practices for securing sensitive data and is part of a comprehensive security strategy.

ISO 27001 - Annex A.10 - Cryptography
ISO 27001 Annex A.10 - Cryptography | ISMS.online
ISO 27001 cryptographic controls policy | What needs to be included?

NEW QUESTION # 162
Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a j